Practitioner's Docket No. 61230 (47762)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Keisuke TAKEMORI et al.

U.S.S.N.: Not Yet Assigned Art Unit: Not Yet assigned

FILED: April 14, 2004 Examiner: Not Yet Assigned

FOR: IDS LOG ANALYSIS SUPPORT APPARATUS, IDS LOG ANALYSIS SUPPORT METHOD AND IDS LOG ANALYSIS SUPPORT PROGRAM

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF CERTIFIED COPIES

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence and the documents referred to as attached therein are being deposited with the United States Postal Service on this date **April 14, 2004** in an envelope as "Express Mail Post Office Addressee," Mailing Label No. **EV438971292US**, addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

By: Michelle P. Chicos
Michelle P. Chicos

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country:	Japan
Application Number:	2003-112414
Filing Date:	April 17, 2003

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 C.F.R.section 1.4(f) (emphasis added).

SIGNATURE OF PRACTITIONER

Date: April 14, 2004

Steven M. Jensen (Reg. No. 42,693)
EDWARDS & ANGELL, LLP
P. O. Box 55874
Boston, MA 02205

Tel. No. (617) 439-4444
Fax. No. (617) 439-4170

NOTE: "The claim to priority need be in no special form and may be made by the attorney or agent, if the foreign application is referred to in the oath or declaration, as required by section 1.63." 37 C.F.R. section 1.55(a).

OSP15798
US15798 1/1

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月１７日

出願番号
Application Number: 特願２００３－１１２４１４

[ST. 10/C]: [ＪＰ２００３－１１２４１４]

出願人
Applicant(s): ＫＤＤＩ株式会社

２００４年　３月２５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０２４８５１

【書類名】　特許願

【整理番号】　J11835A1

【提出日】　平成15年 4月17日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 13/00

G06F 11/34

G06F 15/00

【発明の名称】　ＩＤＳログ分析支援装置、ＩＤＳログ分析支援方法及びＩＤＳログ分析支援プログラム

【請求項の数】　30

【発明者】

【住所又は居所】　埼玉県上福岡市大原２丁目１番１５号　株式会社ケイディーディーアイ研究所内

【氏名】　竹森　敬祐

【発明者】

【住所又は居所】　埼玉県上福岡市大原２丁目１番１５号　株式会社ケイディーディーアイ研究所内

【氏名】　中尾　康二

【特許出願人】

【識別番号】　000208891

【氏名又は名称】　ＫＤＤＩ株式会社

【代理人】

【識別番号】　100101465

【弁理士】

【氏名又は名称】　青山　正和

【代理人】

【識別番号】　100064908

【弁理士】

【氏名又は名称】　志賀　正武

【選任した代理人】

【識別番号】　100089037

【弁理士】

【氏名又は名称】　渡邊　隆

【手数料の表示】

【予納台帳番号】　008707

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0007395

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ＩＤＳログ分析支援装置、ＩＤＳログ分析支援方法及びＩＤＳログ分析支援プログラム

【特許請求の範囲】

【請求項１】　通信網に接続された侵入検知システムのログを収集するログ収集部と、

前記ログ収集部で収集されたログについて保存して管理するデータベースと、

前記データベースで管理されているログについて統計をとり分析処理するログ分析部とを有することを特徴とするＩＤＳ分析支援装置。

【請求項２】　前記ログ分析部は、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログと、前記ログにおける該保護対象側から該非保護対象側へのアクセスログである外向きログとを逐次比較し、該比較結果における一致の程度を示す類似度を逐次算出し、該類似度に基づいて異常が生じたか否か判断する内外類似度分析手段を有することを特徴とする請求項１に記載のＩＤＳ分析支援装置。

【請求項３】　前記ログ分析部は、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名を検知対象として、該国名の検知頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析手段を有することを特徴とする請求項１又は２に記載のＩＤＳ分析支援装置。

【請求項４】　前記ログ分析部は、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名を検知対象として、普段検知されていない該国名の検知頻度が増加したときに、異常が生じたと判断するアクセス国分析手段を有することを特徴とする請求項１又は２に記載のＩＤＳ分析支援装置。

【請求項５】　前記ログ分析部は、

前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信先が属する国名を検知対象として、該国名の検知頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析手段を有することを特徴とする請求項１又は２に記載のＩＤＳ分析支援装置。

【請求項６】　前記ログ分析部は、

前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信先が属する国名を検知対象として、普段検知されていない該国名の検知頻度が増加したときに、異常が生じたと判断するアクセス国分析手段を有することを特徴とする請求項１又は２に記載のＩＤＳ分析支援装置。

【請求項７】　前記ログ分析部は、

前記ログにおける所望の単位期間に含まれる所定の事象の数である短期事象数と、複数の該単位期間についての短期事象数の平均値とを比較し、該平均値に対する該短期事象数の比率に基づいて異常が生じたか否か判断する比率分析手段を有することを特徴とする請求項１乃至６のいずれか一項に記載のＩＤＳ分析支援装置。

【請求項８】　前記ログ分析部は、

前記ログにおける所望の単位期間に含まれる所定の事象の数である短期事象数と、複数の該単位期間についての短期事象数の平均値と、該複数の単位期間についての短期事象数についての標準偏差値とを算出し、検査対象の短期事象数と該平均値との差を該標準偏差値で除算した結果を用いて、異常が生じたか否かを判断する閾値学習分析手段を有することを特徴とする請求項１乃至７のいずれか一項に記載のＩＤＳ分析支援装置。

【請求項９】　前記通信網には、複数の前記侵入検知システムが接続されており、

前記複数の侵入検知システムは、それぞれ異なる保護対象をもっており、

前記ログ分析部は、前記複数の侵入検知システムにおける一つの侵入検知システムである注目侵入検知システムの前記ログの特徴である注目プロファイルと、

該複数の侵入検知システムにおける該注目侵入検知システム以外の侵入検知システム全体についてのログの特徴である総合プロファイルとを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断するＩＤＳ比較手段を有することを特徴とする請求項１乃至８のいずれか一項に記載のＩＤＳ分析支援装置。

【請求項１０】　前記ＩＤＳ比較手段は、前記注目プロファイルの時間経過にともなう変動状況と、前記総合プロファイルの時間経過にともなう変動状況とを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断する変動状況比較機能を有することを特徴とする請求項９に記載のＩＤＳ分析支援装置。

【請求項１１】　通信網に接続された侵入検知システムのログを定期的に収集し、

前記ログについてデータベースに保存して管理し、

前記データベースで管理されているログについて統計をとって分析処理することを特徴とするＩＤＳログ分析支援方法。

【請求項１２】　前記分析処理は、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログと、前記ログにおける該保護対象側から該非保護対象側へのアクセスログである外向きログとを逐次比較し、該比較結果における一致の程度を示す類似度を用いて、異常が生じたか否か判断する内外類似度分析処理を有することを特徴とする請求項１１に記載のＩＤＳ分析支援方法。

【請求項１３】　前記分析処理は、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名の出現頻度について逐次検出し、該国名の検知頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析処理を有することを特徴とする請求項１１又は１２に記載のＩＤＳ分析支援方法。

【請求項１４】　前記分析処理は、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名の出現頻度について逐次検出し、普段検知されていない該国名の出現頻度が増加したときに、異常が生じたと判断するアクセス国分析処理を有することを特徴とする請求項１１又は１２に記載のＩＤＳ分析支援方法。

【請求項１５】　前記分析処理は、

前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信先が属する国名の出現頻度について逐次検出し、該国名の検知頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析処理を有することを特徴とする請求項１１又は１２に記載のＩＤＳ分析支援方法。

【請求項１６】　前記分析処理は、

前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信先が属する国名の出現頻度について逐次検出し、普段検知されていない該国名の検知頻度が増加したときに、異常が生じたと判断するアクセス国分析処理を有することを特徴とする請求項１１又は１２に記載のＩＤＳ分析支援方法。

【請求項１７】　前記分析処理は、

前記ログにおける所望の期間に含まれる所定の事象の数である短期事象数と、該所望の期間よりも長い期間に含まれる該所定の事象の数である長期事象数との比率を逐次算出し、該比率に基づいて異常が生じたか否かを判断する比率分析処理を有することを特徴とする請求項１１乃至１６のいずれか一項に記載のＩＤＳ分析支援方法。

【請求項１８】　前記分析処理は、

前記ログにおける所望の単位期間に含まれる所定の事象の数である短期事象数と、複数の該単位期間についての短期事象数の平均値と、該複数の単位期間についての短期事象数についての標準偏差値とを算出し、検査対象の短期事象数と該

平均値との差を該標準偏差値で除算した結果を用いて、異常が生じたか否かを判断する閾値学習分析処理を有することを特徴とする請求項１１乃至１７のいずれか一項に記載のＩＤＳ分析支援方法。

【請求項１９】　前記通信網には、複数の前記侵入検知システムが接続されており、

前記複数の侵入検知システムは、それぞれ異なる保護対象をもっており、

前記分析処理は、前記複数の侵入検知システムにおける一つの侵入検知システムである注目侵入検知システムの前記ログの特徴である注目プロファイルと、該複数の侵入検知システムにおける該注目侵入検知システム以外の侵入検知システム全体についてのログの特徴である総合プロファイルとを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断するＩＤＳ比較処理を有することを特徴とする請求項１１乃至１８のいずれか一項に記載のＩＤＳ分析支援方法。

【請求項２０】　前記ＩＤＳ比較処理は、前記注目プロファイルの時間経過にともなう変動状況と、前記総合プロファイルの時間経過にともなう変動状況とを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断する変動状況比較処理を有することを特徴とする請求項１９に記載のＩＤＳ分析支援方法。

【請求項２１】　通信網に接続された侵入検知システムのログを分析するＩＤＳログ分析支援プログラムにおいて、

前記侵入検知システムから前記ログを収集するログ収集ステップと、

前記ログ収集ステップで収集されたログについて保存して管理するデータベース化ステップと、

前記データベース化ステップで管理されているログについて統計をとり分析処理するログ分析ステップとをコンピュータに実行させることを特徴とするＩＤＳログ分析支援プログラム。

【請求項２２】　前記ログ分析ステップは、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログと、前記ログにおける該保護

対象側から該非保護対象側へのアクセスログである外向きログとを逐次比較し、該比較結果における一致の程度を示す類似度を用いて、異常が生じたか否か判断する内外類似度分析ステップを有することを特徴とする請求項２１に記載のＩＤＳ分析支援プログラム。

【請求項２３】　前記ログ分析ステップは、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名の出現頻度について逐次検出し、該国名の出現頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析ステップを有することを特徴とする請求項２１又は２２に記載のＩＤＳ分析支援プログラム。

【請求項２４】　前記ログ分析ステップは、

前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名の出現頻度について逐次検出し、普段検知されていない該国名の出現頻度が増加したときに、異常が生じたと判断するアクセス国分析ステップを有することを特徴とする請求項２１又は２２に記載のＩＤＳ分析支援プログラム。

【請求項２５】　前記ログ分析ステップは、

前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信元が属する国名の出現頻度について逐次検出し、該国名の出現頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析ステップを有することを特徴とする請求項２１又は２２に記載のＩＤＳ分析支援プログラム。

【請求項２６】　前記ログ分析ステップは、

前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信元が属する国名の出現頻度について逐次検出し、普段検知されていない該国名の出現頻度が増加したときに、異常が生じたと判断するアクセス国分析ステップを有することを特徴とす

る請求項２１又は２２に記載のＩＤＳ分析支援プログラム。

【請求項２７】　前記ログ分析ステップは、

前記ログにおける所望の期間に含まれる所定の事象の数である短期事象数と、該所望の期間よりも長い期間に含まれる該所定の事象の数である長期事象数との比率を逐次算出し、該比率に基づいて異常が生じたか否かを判断する比率分析ステップを有することを特徴とする請求項２１乃至２６のいずれか一項に記載のＩＤＳ分析支援プログラム。

【請求項２８】　前記ログ分析ステップは、

前記ログにおける所望の単位期間に含まれる所定の事象の数である短期事象数と、複数の該単位期間についての短期事象数の平均値と、該複数の単位期間についての短期事象数についての標準偏差値とを算出し、検査対象の短期事象数と該平均値との差を該標準偏差値で除算した結果を用いて、異常が生じたか否かを判断する閾値学習分析ステップを有することを特徴とする請求項２１乃至２７のいずれか一項に記載のＩＤＳ分析支援プログラム。

【請求項２９】　前記通信網には、複数の前記侵入検知システムが接続されており、

前記複数の侵入検知システムは、それぞれ異なる保護対象をもっており、

前記ログ分析ステップは、前記複数の侵入検知システムにおける一つの侵入検知システムである注目侵入検知システムの前記ログの特徴である注目プロファイルと、該複数の侵入検知システムにおける該注目侵入検知システム以外の侵入検知システム全体についてのログの特徴である総合プロファイルとを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断するＩＤＳ比較ステップを有することを特徴とする請求項２１乃至２８のいずれか一項に記載のＩＤＳ分析支援プログラム。

【請求項３０】　前記ＩＤＳ比較ステップは、前記注目プロファイルの時間経過にともなう変動状況と、前記総合プロファイルの時間経過にともなう変動状況とを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断する変動状況比較ステップを有することを特徴とする請求項２９に記載のＩＤＳ分析支援プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、侵入検知システム（ＩＤＳ：Intrusion Detection System）から出力されるログの分析について支援するＩＤＳログ分析支援装置、ＩＤＳログ分析支援方法及びＩＤＳログ分析支援プログラムに関する。

【０００２】

【従来の技術】

近年、ネットワークシステムに対する攻撃監視のためにネットワーク型ＩＤＳ（以下、単にＩＤＳという）を導入するサイトが増えている。一般にＩＤＳは、トラヒックを監視して攻撃を検知する検知エンジンと、そのログを集中管理して分析する管理コンソールからなる。多くの検知エンジンは、ネットワーク上を流れるパケットとシグネチャと呼ばれる攻撃パターンファイルとを単純に比較してマッチングするものがあればログを出力する。管理コンソールは、出力されたログを時系列順に表示する機能及び簡単な統計処理を行う機能を持っている。

【０００３】

また、従来においては、コンピュータの稼働状況を示すログ情報の解析作業に要する時間を減少させ、種々のデータ形式とファイル・システム上の偏在性とを有するログ情報を統合し、既知の異常ではない異常を示すログ情報を抽出することを目的としたログ情報解析装置が考え出されている。このログ情報解析装置はシステム管理者が文字による膨大な量のログ情報を棒グラフのように表示させて注目すべき情報を迅速に把握しようとするものである（例えば、特許文献１参照）。

【０００４】

【特許文献１】

特開２００１－３５６９３９号公報

【０００５】

【発明が解決しようとする課題】

しかしながら、上記特許文献１に記載されたログ情報解析装置では、ホストか

ら出力されるログデータに注目しており、分析手法として「単語出現頻度」又は「テキスト長」に関する異常性をビジュアル的に提供するものであるので、以下の問題点を有している。

【０００６】

すなわち、上記特許文献１に記載されたログ情報解析装置は、ネットワークへの攻撃を監視するＩＤＳのログ解析に適用することができない。また、上記特許文献１に記載されたログ情報解析装置は、分析アルゴリズムの数学的手法が明確でなく、客観的な数値として出力することができない。また、上記特許文献１に記載されたログ情報解析装置は、攻撃ログに特化したものではないので、いつもとは異なる正規の行為をも検出してしまう。

【０００７】

そして、従来においては、実際には導入されたＩＤＳがそのまま放置され、有効に活用されないケースが多々ある。この問題は、主に、誤検知、多重検知、セキュリティ対策済みのシステムに対する攻撃検知など、大量に出力される冗長なログを分析しきれないことが原因となっている。また、この問題は、単純マッチング型のＩＤＳの場合、攻撃の意図や成否の判定が困難であるということも原因となっている。

【０００８】

既存のＩＤＳには、単純な統計を行う機能はあるものの、統計値がどの程度危険なものであるかの判断を、運用者の経験と主観に依存している。その他、利用するＩＤＳにより出力されるログの形式が異なり、攻撃に対するＩＤＳの反応はまちまちである。また、従来においては、監視に利用するＩＤＳ毎にログ出力の特徴を把握しなければならいという問題もある。このように、従来においては、様々なＩＤＳから出力される大量のログからの中から、普段と異なる痕跡を客観的に抽出することができない。

【０００９】

また、大量に出力されるログをフィルタリングする手法として、監視する必要のないシグネチャを検知エンジンから削除するポリシーチューニング手法、及び管理コンソール上でネットワークの脆弱性に関する監査データを用いて、対策の

施されたシステムに対する攻撃ログを分析対象から削除するフィルタリング手法などが考え出されている。

【００１０】

しかし、上記ポリシーチューニング手法では、ポリシーチューニングに掛かるコスト、及び誤って重要なシグネチャを外してしまう人為的なミス、さらには様々な角度から攻撃を試みる侵入者の分析には一見無駄とも思われる多くのログが必要となってくるという問題がある。また、上記フィルタリング手法では、誤って未監査のシステムを設置してしまう人為的なミスや、システム導入のたびに監査に掛かるコストが問題となる。

【００１１】

本発明は、上述した事情に鑑みてなされたもので、様々なＩＤＳより大量に出力されたログの中から、普段と異なるログを抽出して、その異常度を客観的に評価することができるＩＤＳログ分析支援装置、ＩＤＳログ分析支援方法及びＩＤＳログ分析支援プログラムの提供を目的とする。

【００１２】

【課題を解決するための手段】

上記の目的を達成するために、請求項１記載の発明は、通信網に接続された侵入検知システムのログを収集するログ収集部と、前記ログ収集部で収集されたログについて保存して管理するデータベースと、前記データベースで管理されているログについて統計をとり分析処理するログ分析部とを有することを特徴とするＩＤＳログ分析支援装置を提供する。

本発明によれば、侵入検知システムから逐次的に多量に出力されるログについて統計分析をするので、例えばログにおける長期間の特徴（例えば平均値など）に対する短期間の特徴の差を異常値として、かかるログを客観的に評価することができる。

【００１３】

また、請求項２記載の発明は、前記ログ分析部が、前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログと、前記ログにおける該保護対象側から該非保護対象側へ

のアクセスログである外向きログとを逐次比較し、該比較結果における一致の程度を示す類似度を逐次算出し、該類似度に基づいて異常が生じたか否か判断する内外類似度分析手段を有することを特徴とする。

本発明によれば、例えばインターネットなどから侵入検知システムの保護対象に向かってくるアクセスのログである内向きログと、その保護対象からインターネットなどの外部へ向かうアクセスのログである外向きログとの類似度について逐次判断する。通常では内向きログはワームなどの攻撃事象が多く存在し、外向きログは危険事象が比較的少ない。そこで、本発明によれば、例えばかかる類似度が急に一致していきた場合などは保護対象がワームなどに感染したおそれがあると判断することができる。

【００１４】

また、請求項３記載の発明は、前記ログ分析部が、前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名を検知対象として、該国名の検知頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析手段を有することを特徴とする。

本発明によれば、かかる送信元の国名を逐次分析するので、新たな攻撃の流行などを把握することができ、異常事態が生じたことを客観的にかつ迅速に検出することができる。これは、侵入検知システムの保護対象側にアクセスしてくる送信元の国は一般にその保護対象が属している国と同一のものが多いので、例えば外国からのアクセスが急に増加した場合は異常事態が生じたおそれがあると判断することができる。

【００１５】

また、請求項４記載の発明は、前記ログ分析部が、前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名を検知対象として、普段検知されていない該国名の検知頻度が増加したときに、異常が生じたと判断するアクセス国分析手段を有することを特徴とする。

本発明によれば、かかる送信元の国名を逐次分析するので、新たな攻撃の流行

などを把握することができ、異常事態が生じたことを客観的にかつ迅速に検出することができる。

【００１６】

また、請求項５記載の発明は、前記ログ分析部が、前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信先が属する国名を検知対象として、該国名の検知頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析手段を有することを特徴とする。

本発明によれば、保護対象がウィルスに感染したこと及び踏み台ホストになっていることなどを検知することができる。これは例えば保護対象から外国へのアクセスが急激に増加した場合はウィルスに感染した又は踏み台ホストになった場合が多いからである。

【００１７】

また、請求項６記載の発明は、前記ログ分析部が、前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信先が属する国名を検知対象として、普段検知されていない該国名の検知頻度が増加したときに、異常が生じたと判断するアクセス国分析手段を有することを特徴とする。

本発明によれば、保護対象がウィルスに感染したこと及び踏み台ホストになっていることなどを検知することができる。

【００１８】

また、請求項７記載の発明は、前記ログ分析部が、前記ログにおける所望の単位期間に含まれる所定の事象の数である短期事象数（短期プロファイル）と、複数の該単位期間についての短期事象数の平均値とを比較し、該平均値に対する該短期事象数の比率に基づいて異常が生じたか否か判断する比率分析手段を有することを特徴とする。

本発明によれば、例えば平均値に対する短期事象数の比率が急増した場合は、保護対象に対する攻撃が生じている又は保護対象にワームが感染したと判断することができる。また、例えば平均値に対する短期事象数の比率が減少した場合は

保護対象（ホストや内部ネットワークなど）の一部機能が停止したと判断することができる。

【００１９】

また、請求項８記載の発明は、前記ログ分析部が、前記ログにおける所望の単位期間に含まれる所定の事象の数である短期事象数と、複数の該単位期間についての短期事象数の平均値と、該複数の単位期間についての短期事象数についての標準偏差値とを算出し、検査対象の短期事象数と該平均値との差を該標準偏差値で除算した結果を用いて、異常が生じたか否かを判断する閾値学習分析手段を有することを特徴とする。

本発明によれば、侵入検知システムのログについて標準偏差値などを算出してその標準偏差を用いて異常が生じたか否か判断するので、ログにおける所望の事象数（データ）のばらつき具合を考慮して異常が生じたか否かを判断することができる。

【００２０】

また、請求項９記載の発明は、前記通信網には複数の前記侵入検知システムが接続されており、前記複数の侵入検知システムは、それぞれ異なる保護対象をもっており、前記ログ分析部は、前記複数の侵入検知システムにおける一つの侵入検知システムである注目侵入検知システムの前記ログの特徴である注目プロファイルと、該複数の侵入検知システムにおける該注目侵入検知システム以外の侵入検知システム全体についてのログの特徴である総合プロファイルとを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断するＩＤＳ比較手段を有することを特徴とする。

本発明によれば、例えば複数のＩＤＳがそれぞれ異なる保護対象（イントラネットなど）を監視しているときに、その複数のＩＤＳの保護対象全体（あるネットワーク全体など）のうちの特定の保護対象（イントラネットなど）に異常が生じたか否かを判断することができる。すなわち、従来は１個のＩＤＳ単体のログについて判断していたものを、本発明によれば、複数のＩＤＳのログ全体とそのうちの一つのＩＤＳのログとを比較して、各ＩＤＳのログの異常度を判断することができる。

【００２１】

また、請求項１０記載の発明は、前記ＩＤＳ比較手段が、前記注目プロファイルの時間経過にともなう変動状況と、前記総合プロファイルの時間経過にともなう変動状況とを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断する変動状況比較機能を有することを特徴とする。

本発明によれば、例えば総合プロファイルの変動状況が安定しているときに、注目プロファイルの変動状況が所定事項について急激に増加している場合、あるＩＤＳの保護対象がワームに感染したおそれがあると判断することができる。

【００２２】

また、上記の目的を達成するために、請求項１１記載の発明は、通信網に接続された侵入検知システムのログを定期的に収集し、前記ログについてデータベースに保存して管理し、前記データベースで管理されているログについて統計をとって分析処理することを特徴とする。

【００２３】

また、請求項１２記載の発明は、前記分析処理が、前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログと、前記ログにおける該保護対象側から該非保護対象側へのアクセスログである外向きログとを逐次比較し、該比較結果における一致の程度を示す類似度を用いて、異常が生じたか否か判断する内外類似度分析処理を有することを特徴とする。

【００２４】

また、請求項１３記載の発明は、前記分析処理が、前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名の出現頻度について逐次検出し、該国名の検知頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析処理を有することを特徴とする。

【００２５】

また、請求項１４記載の発明は、前記分析処理が、前記ログにおける前記侵入

検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名の出現頻度について逐次検出し、普段検知されていない該国名の出現頻度が増加したときに、異常が生じたと判断するアクセス国分析処理を有することを特徴とする。

【００２６】

また、請求項１５記載の発明は、前記分析処理が、前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信先が属する国名の出現頻度について逐次検出し、該国名の検知頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析処理を有することを特徴とする。

【００２７】

また、請求項１６記載の発明は、前記分析処理が、前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信先が属する国名の出現頻度について逐次検出し、普段検知されていない該国名の検知頻度が増加したときに、異常が生じたと判断するアクセス国分析処理を有することを特徴とする。

【００２８】

また、請求項１７記載の発明は、前記分析処理が、前記ログにおける所望の期間に含まれる所定の事象の数である短期事象数と、該所望の期間よりも長い期間に含まれる該所定の事象の数である長期事象数との比率を逐次算出し、該比率に基づいて異常が生じたか否かを判断する比率分析処理を有することを特徴とする。

【００２９】

また、請求項１８記載の発明は、前記分析処理が、前記ログにおける所望の単位期間に含まれる所定の事象の数である短期事象数と、複数の該単位期間についての短期事象数の平均値と、該複数の単位期間についての短期事象数についての標準偏差値とを算出し、検査対象の短期事象数と該平均値との差を該標準偏差値で除算した結果を用いて、異常が生じたか否かを判断する閾値学習分析処理を有

することを特徴とする。

【００３０】

また、請求項１９記載の発明は、前記通信網には、複数の前記侵入検知システムが接続されており、前記複数の侵入検知システムは、それぞれ異なる保護対象をもっており、前記分析処理は、前記複数の侵入検知システムにおける一つの侵入検知システムである注目侵入検知システムの前記ログの特徴である注目プロファイルと、該複数の侵入検知システムにおける該注目侵入検知システム以外の侵入検知システム全体についてのログの特徴である総合プロファイルとを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断するＩＤＳ比較処理を有することを特徴とする。

【００３１】

また、請求項２０記載の発明は、前記ＩＤＳ比較処理が、前記注目プロファイルの時間経過にともなう変動状況と、前記総合プロファイルの時間経過にともなう変動状況とを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断する変動状況比較処理を有することを特徴とする。

【００３２】

また、上記の目的を達成するために、請求項２１記載の発明は、通信網に接続された侵入検知システムのログを分析するＩＤＳログ分析支援プログラムにおいて、前記侵入検知システムから前記ログを収集するログ収集ステップと、前記ログ収集ステップで収集されたログについて保存して管理するデータベース化ステップと、前記データベース化ステップで管理されているログについて統計をとり分析処理するログ分析ステップとをコンピュータに実行させることを特徴とする。

【００３３】

また、請求項２２記載の発明は、前記ログ分析ステップが、前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログと、前記ログにおける該保護対象側から該非保護対象側へのアクセスログである外向きログとを逐次比較し、該比較結果における一致の程度を示す類似度を用いて、異常が生じたか否か判断する内外類似度分析

ステップを有することを特徴とする。

【００３４】

また、請求項２３記載の発明は、前記ログ分析ステップが、前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名の出現頻度について逐次検出し、該国名の出現頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析ステップを有することを特徴とする。

【００３５】

また、請求項２４記載の発明は、前記ログ分析ステップが、前記ログにおける前記侵入検知システムの非保護対象側から該侵入検知システムの保護対象側へのアクセスログである内向きログの送信元が属する国名の出現頻度について逐次検出し、普段検知されていない該国名の出現頻度が増加したときに、異常が生じたと判断するアクセス国分析ステップを有することを特徴とする。

【００３６】

また、請求項２５記載の発明は、前記ログ分析ステップが、前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信元が属する国名の出現頻度について逐次検出し、該国名の出現頻度に順位を付け、普段検知されている該国名の該順位に変動があったときに、異常が生じたと判断するアクセス国分析ステップを有することを特徴とする。

【００３７】

また、請求項２６記載の発明は、前記ログ分析ステップが、前記ログにおける前記侵入検知システムの保護対象側から該侵入検知システムの非保護対象側へのアクセスログである外向きログの送信元が属する国名の出現頻度について逐次検出し、普段検知されていない該国名の出現頻度が増加したときに、異常が生じたと判断するアクセス国分析ステップを有することを特徴とする。

【００３８】

また、請求項２７記載の発明は、前記ログ分析ステップが、前記ログにおける

所望の期間に含まれる所定の事象の数である短期事象数と、該所望の期間よりも長い期間に含まれる該所定の事象の数である長期事象数との比率を逐次算出し、該比率に基づいて異常が生じたか否かを判断する比率分析ステップを有することを特徴とする。

【００３９】

また、請求項２８記載の発明は、前記ログ分析ステップが、前記ログにおける所望の単位期間に含まれる所定の事象の数である短期事象数と、複数の該単位期間についての短期事象数の平均値と、該複数の単位期間についての短期事象数についての標準偏差値とを算出し、検査対象の短期事象数と該平均値との差を該標準偏差値で除算した結果を用いて、異常が生じたか否かを判断する閾値学習分析ステップを有することを特徴とする。

【００４０】

また、請求項２９記載の発明は、前記通信網には、複数の前記侵入検知システムが接続されており、前記複数の侵入検知システムは、それぞれ異なる保護対象をもっており、前記ログ分析ステップは、前記複数の侵入検知システムにおける一つの侵入検知システムである注目侵入検知システムの前記ログの特徴である注目プロファイルと、該複数の侵入検知システムにおける該注目侵入検知システム以外の侵入検知システム全体についてのログの特徴である総合プロファイルとを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断するＩＤＳ比較ステップを有することを特徴とする。

【００４１】

また、請求項３０記載の発明は、前記ＩＤＳ比較ステップが、前記注目プロファイルの時間経過にともなう変動状況と、前記総合プロファイルの時間経過にともなう変動状況とを比較し、該比較結果に所定値以上の差違があったときに、異常が生じたと判断する変動状況比較ステップを有することを特徴とする。

【００４２】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態について説明する。

図１は本発明の実施の形態に係るＩＤＳログ分析支援システムの適用形態及び

構成を示す模式図である。

本実施形態のＩＤＳログ分析支援システム１は、インターネットに接続された複数のサイトＡ，Ｂ，Ｃにそれぞれ導入されたＩＤＳ５０からのログ５１を収集して管理及び分析するものである。各サイトＡ，Ｂ，Ｃには、WWWサーバ及びメールサーバなどの各種サーバ６０やクライアント・パソコンなどが配置されている。そして、サイトＡ，Ｂ，ＣがＩＤＳ５０の保護対象である。

【００４３】

ＩＤＳログ分析支援システム１（ＩＤＳログ分析支援装置）は、ログ収集部１０と、データベース２０と、ログ分析部３０とを備える。ログ収集部１０は、各サイトＡ，Ｂ，ＣそれぞれのＩＤＳ５０から逐次出力されるログ５１を定期的に収集するものである。データベース２０は、ログ収集部１０で収集されたログ５１について保存及び管理するものである。ログ分析部３０は、データベース２０で管理されているログ５１について統計的な分析処理をするものである。

【００４４】

ログ収集部は、ＩＤＳ５０の管理コンソール上のログ５１及び検知エンジンと管理コンソールが統合されたＩＤＳ５０上のログ５１を、暗号化パスを通じて定期的に収集を行い、統一されたフォーマットを持つデータベース２０に保存する。ログ分析部３０は、データベース２０で管理するログに対して各種分析処理を行う。

【００４５】

次に、ＩＤＳログ分析支援システム１が対象とするログの一例について、図２を参照して説明する。ＩＤＳログ分析支援システム１が対象とするログとしては例えばSnort、 ICEcap、SiteProtector、Secure ＩＤＳの4つを挙げることができる。図２はSnortのログであるAlertファイルの内容を示す表示例図である。

【００４６】

図２に示すように、各ログは、［＊＊］で囲まれたシグネチャIDとシグネチャ名で始まり、次の［＊＊］の前までである。ログには、検知日時、Source IP/Port（送信元）、Destination IP/Port（送信先）、通信プロトコルなどの情報が含まれている。Snortには、Alertファイル以外にも、情報収集に関するScanログ

ファイルが出力される。他の三つのＩＤＳログ（ICEcap、SiteProtector、Secure ＩＤＳ）についても、Snortログと同様な項目を持っている。

【００４７】

（分析パラメータとＤＢ設計）

次に、データベース２０の設計について説明する。各種のＩＤＳ５０から出力されるログ５１に対して、統一した分析手法を適用するために、統合型のデータベース２０を設計する。これは、ＩＤＳ５０の種類毎について分析スキルの必要性を無くして、利用し易いＩＤＳログ分析支援システムを提供するためである。

【００４８】

各サイトＡ，Ｂ，Ｃに対する各種攻撃の異常度を評価するために、注目すべきログ項目を以下に列挙する。各種攻撃とは、ターゲットホスト検索のための情報収集（レベル１）、ターゲットホストへの侵入の試み（レベル２）、侵入後の権限昇格・消去・改ざん・盗難・隠蔽（レベル３）、ターゲットホストを踏み台としての第三者への攻撃（レベル４）、ＤＤｏＳ攻撃（レベル５）が挙げられる。

【００４９】

まず、注目すべきログ項目としては、ＩＤＳ５０の運用者がどの検知エンジンでどのような攻撃を検知したのかを知るために、「Sensor ID」及び「シグネチャ名」を、データベース２０の項目とする。

次に、検出されたシグネチャの順序関係／攻撃時間長／攻撃間のタイミング等の把握及び各種統計処理の実施のために、「時刻」に注目し、これをデータベース２０の項目とする。

そして、攻撃元（Source）と攻撃対象（Destination）を知るために、「Source IP/port」及び「Destination IP/Port」に注目し、これをデータベース２０の項目とする。

その他、攻撃を行った際の「通信プロトコル」及び攻撃と判定したときの「理由（攻撃検知Parameter）」等も分析するために、これをデータベース２０の項目とする。

【００５０】

上記要素（項目）を持つ統合ＤＢであるデータベース２０におけるテーブルの

フォーマットの一例を図３から図５に示す。図３は事象テーブルであり、図４はシグネチャテーブルであり、図５は事象パラメータテーブルである。

【００５１】

（統計分析）

次に、ログ分析部３０が行うログの統計分析について詳細に説明する。

ＩＤＳのログについて運用者（ログ分析部３０）が分析する項目としては、「Source IP/Port」、「Destination IP/Port」及び「シグネチャ名」が挙げられる。これらの項目に対して時間軸に対する事象数の統計分析として、統計値パターン分析モデル（内外類似度分析モデル、アクセス国分析モデル）、比率分析モデル（手段）、閾値学習モデル（手段）を適用する。

【００５２】

統計値パターン分析モデルは、時間軸に対する事象数の統計値のパターンに注目した分析を行うものである。そして、統計値パターン分析モデルとしては、内外類似度分析モデル（手段）及びアクセス国分析モデル（手段）を適用する。

【００５３】

＜内外類似度分析モデル（手段）＞

保護対象の外部であるインターネットから内部（サイトＡ，Ｂ，Ｃ内）のイントラネット（保護対象）などへのアクセスには、ワームなどによる攻撃が多く含まれている。逆に、イントラネットからインターネットへのアクセスには、ワームによる攻撃は通常無いと考えられる。このように、インターネットからのアクセスを汚れたトラヒックとみなしたとき、イントラネットからのアクセスが、どの程度、外部の汚れたトラヒックに類似しているか（類似度）を指標として、その類似度について検出して判断する内外類似度分析モデル（手段）をログ分析部３０に設け、これによりワームへの感染ホストや踏み台化ホストを検出する。

【００５４】

例えば、類似度について逐次検査し、類似度が通常の状態（平均的な値）から急激に変動したときに、攻撃されている又は攻撃されたと判断する。すなわち、まだ攻撃されていない通常状態では、インターネットからイントラネットへのトラヒックとイントラネットからインターネットへのトラヒックは大きく異なって

いる。一方、攻撃されたときは、インターネットからイントラネットへのトラヒックとイントラネットからインターネットへのトラヒックとは、ともに汚れた状態となり急激に一致してくる。これにより、攻撃されると、上記類似度が急激に変動するので、類似度を逐次検査することで、攻撃されたことを迅速に検出することができる。

【００５５】

ワーム感染ホストの検知手法としては、外部から内部へ攻撃された直後に、内部から外部へ同じシグネチャ名や同じ送信先ポート（Destination Port）へ攻撃することに注目する。また、攻撃元は、ＩＰアドレスにより特定することができる。

【００５６】

＜アクセス国分析モデル（手段）＞

普段、イントラネット（保護対象）へアクセスしてくる国は、そのイントラネットが属している国と同一のものが多いか、もしくは、ある特定の国に集中している。逆にイントラネットからインターネットへのアクセスも同じような傾向になる。

【００５７】

インターネット上で新たな攻撃が流行り始めたときには、普段アクセスしてくる国とは異なる国からのアクセスが増加する。これは、多くのワームが、攻撃先IPをランダムに選択する特徴があることによる。また、イントラネット上に踏み台となったホストがあると、アクセスする国の傾向も変化する。よって、国に関する長期プロファイル（長期間の統計値又はデータ）と短期プロファイル（短期間の統計値又はデータ）の差異をログ分析部３０で分析することで、インターネット上での新たな攻撃の予兆、及びイントラネット上での踏み台ホストの把握が可能になる。

【００５８】

そこで、ログ分析部３０は、ログ５１におけるインターネットからイントラネットへのアクセス（内向きログ）の送信元が属する国名を検知対象として、その国名の検知頻度に順位を付けて普段検知されている国名の順位に変動があったと

きに、又は、普段検知されていない国名の検知頻度が増加したときに、異常が生じたと判断するアクセス国分析手段を備えることとする。これにより、インターネット上での新たな攻撃の流行などの把握が可能になる。

【００５９】

また、ログ分析部３０は、ログ５１におけるイントラネットからインターネットへのアクセス（外向きログ）の送信先が属する国名を検知対象として、その国名の検知頻度に順位を付けて普段検知されている国名の順位に変動があったときに、又は、普段検知されていない国名の検知頻度が増加したときに、異常が生じたと判断するアクセス国分析手段を備えることとする。これにより、イントラネットがウィルスに感染したこと及びイントラネット内に踏み台ホストが作られたことなどを検知することができる。

【００６０】

＜初検出モデル＞

上記統計値パターン分析モデルの一つとして以下に示す初検出モデル（手段）をログ分析部３０に設けてもよい。

微かに残る痕跡を追うためには、多量のログ５１の中から初めて検知された事象に注目することは重要である。そもそも長期プロファイルにおいて一度も検知されない事象については、各種統計分析を適用することはできない。そこで、ログ分析部３０に初検出モデル（手段）を設けて、過去の長期プロファイルにおいて検出されていないもので、短期プロファイルで新たに検出された事象に注目する。

【００６１】

＜比例分析モデル（手段）＞

次に、ログ分析部３０に設けられている比率分析モデル（手段）について説明する。図６は比率分析モデルについての説明図である。

比率分析モデルは、注目する短期間を単位時間としたときに、短期間に含まれる事象数（＝短期プロファイル）に対する過去の複数の単位時間に含まれる事象数の平均（＝長期プロファイル）の倍率を異常値として評価する手法（手段）である。そこで、ログ分析部３０は、短期プロファイルに対する長期プロファイル

（平均）の倍率（比率）に基づいて異常が生じたか否か判断する比率分析手段を備えている。図６は短期プロファイルを一日としたときの比率分析モデルの様子を示している。

【００６２】

t-1個の単位時間があるとき、n番目の単位時間に含まれる事象数をＥｎとすると、t番目の短期プロファイルに対する長期プロファイルの比率Ｒｔは、下記数１の様に表される。

【００６３】

【数１】

$$R_t = \frac{E_t}{\sum_{n=1}^{t-1} \frac{E_n}{t-1}}$$

【００６４】

Ｒｔ＞1.0の場合

この場合はインターネット上に新たな攻撃が出回り始めたとき、内部ホストがワームに感染したとき、DDoS攻撃を受けたときなど、短期の事象数が急増したことを示している。そこで、比率分析モデルは、内部ホストがワームに感染したこと、DDoS攻撃を受けたことを迅速にかつ正確に検出することができる。

【００６５】

Ｒｔ＜1.0の場合

この場合はフォルスポジティブにより普段から出力され続けていたアラームが急に減少したもしくは無くなってしまったことを示しているので、比率分析モデルはネットワークやホストの停止に関する異常を迅速にかつ正確に見つけることができる。

【００６６】

＜閾値学習モデル＞

次に、ログ分析部３０に設けられている閾値学習モデル（手段）について説明

する。図７は閾値学習モデルについての説明図である。

閾値学習モデルは、平均μと標準偏差σを用いて信頼区間を求める統計手法である。そして、閾値学習モデルでは、統計学における９５％信頼区間を用いるものであり、平均μ及び標準偏差σから求められるＺ値から事象数の異常度を評価する。

【００６７】

本ＩＤＳログ分析支援システム１に当てはめると、ログ分析部３０の閾値学習手段は、単位時間あたりの事象数が、普段検知される事象数に対してどの程度ばらついた値（以後、稀率と呼ぶ）であるかを算出する。標準偏差σを用いることにより、過去のデータのばらつき具合を考慮した評価を行うことができる。そこで、ログ分析部３０の閾値学習手段は、例えば、TCP Port Probeのように普段から誤検知が絶えない攻撃やパスワード辞書攻撃のような時々誤検知さる攻撃などＩＤＳ５０やシグネチャの性格ごとに閾値を学習することができる。

【００６８】

図７では、単位時間を１日として、事象数を横軸にとり、その事象数となった日数を縦軸にとったときの稀率を求める様子を示している。

単位時間がＮ個あるときの事象数の平均μは、下記数２で表される。

【００６９】

【数２】

$$\mu = \frac{\sum_{n=1}^{N} X_n}{N}$$

【００７０】

このときの分散σは、下記数３で表される。

【００７１】

【数３】

$$\sigma = \sqrt{\frac{\sum_{n=1}^{N} (X_n - \mu)^2}{N}}$$

【００７２】

これらの平均μ及び分散σより、Ｎ＋１番目の短期プロファイルの事象数に関すＺＮ＋１スコア（ＺＮ＋１値）は、下記数４で表される。

【００７３】

【数４】

$$Z_{N+1} = \frac{X_{N+1} - \mu}{\sigma}$$

【００７４】

このＺＮ＋１スコアをＺスコア表（正規分布表；Ｚ－table）に対比することで稀率は求まる。

一般に、閾値学習モデルの場合、サンプル数が３０以上にならなければ、正しく信頼区間を求めることができない。よって、単位時間を１日とした場合、３０日以上の事象数をサンプルとして用いることが好ましい。

【００７５】

Ｚ＞０の場合

比率分析モデルの「Ｒｔ＞1.0」の場合と同じである。すなわち、この場合はインターネット上に新たな攻撃が出回り始めたとき、内部ホストがワームに感染したとき、DDoS攻撃を受けたときなど、短期の事象数が急増したことを示している。そこで、閾値学習モデルは、内部ホストがワームに感染したこと、DDoS攻撃を受けたことを迅速にかつ正確に検出することができる。

【００７６】

Ｚ＜０の場合

比率分析モデルの「Ｒｔ＜1.0」の場合と同じである。すなわち、この場合はフォルスポジティブにより普段から出力され続けていたアラームが急に減少したもしくは無くなってしまったことを示しているので、閾値学習モデルはネットワークやホストの停止に関する異常を迅速にかつ正確に見つけることができる。

【００７７】

＜ＩＤＳ比較モデル（手段）＞

ＩＤＳログ分析支援システム１のログ分析部３０は、以下に述べるＩＤＳ比較手段を備えることが好ましい。図１に示すようにインターネットには複数のＩＤＳ５０が接続されており、各ＩＤＳ５０はそれぞれ異なる保護対象（サイトＡ，Ｂ，Ｃ）をもっている。そして、ログ分析部３０は、複数のＩＤＳ５０における一つのＩＤＳ５０（注目侵入検知システム）のログ５１の特徴である注目プロファイルと、複数のＩＤＳ５０における注目侵入検知システム以外のＩＤＳ５０全体についてのログ５１の特徴である総合プロファイルとを比較し、その比較結果に所定値以上の差違があったときに、異常が生じたと判断するＩＤＳ比較手段を有することが好ましい。

【００７８】

このようにすると、例えば複数のＩＤＳ５０がそれぞれ異なる保護対象（サイトＡ，Ｂ，Ｃ）を監視しているときに、その複数のＩＤＳ５０の保護対象全体（サイトＡ，Ｂ，Ｃ）のうちの特定の保護対象（例えばサイトＡ）に異常が生じたか否かを判断することができる。

【００７９】

また、ログ分析部３０のＩＤＳ比較手段は、前記注目プロファイルの時間経過にともなう変動状況と、前記総合プロファイルの時間経過にともなう変動状況とを比較し、その比較結果に所定値以上の差違があったときに、異常が生じたと判断する変動状況比較機能を有することが好ましい。このようにすると、例えば総合プロファイルの変動状況が安定しているときに、注目プロファイルの変動状況が所定事項について急激に増加している場合、あるＩＤＳ５０の保護対象（例え

ばサイトＡ）がワームに感染したおそれがあると判断することができる。

【００８０】

（本実施形態の効果）

次に、本実施形態のＩＤＳログ分析支援システムの効果について説明する。

ログ分析部３０に設けられた比率分析モデル（手段）と閾値学習モデル（手段）は、冗長なログを無視して普段と異なるログを客観的に評価する手法である。そこで、比率分析モデル（手段）と閾値学習モデル（手段）は、冗長なログを削減するためのポリシーチューニングや対策済みフィルタリング等の作業を必要としない（効果１）、及び、普段と異なる特徴を客観的に把握できる（効果２）、という２つの効果を奏することができる。

【００８１】

ログ分析部３０に設けられた初検出モデル（手段）は、多量のログに埋もれがちな僅かな痕跡を抽出する手法であり、出現頻度の低いログを見逃さない（効果３）という効果を奏することができる。

【００８２】

ログ分析部３０に設けられた内外類似度分析モデル（手段）とアクセス国分析モデル（手段）は、ワーム感染及び踏み台化ホストを迅速にかつ正確に検出することができる（効果４）という効果を奏することができる。

【００８３】

次に、各種の攻撃に対する本実施形態のＩＤＳログ分析支援システムの効果について、図８を参照して説明する。図８はＩＤＳ５０の保護対象であるサイトＡ，Ｂ，Ｃに対する各種の攻撃形態を示す説明図である。

【００８４】

一般に攻撃には、ターゲットの脆弱性を探索するものや、弱点を突いて侵入を試みるもの、侵入後に踏み台として利用するものなど、ステップがある。勿論、いきなり脆弱性を突いて侵入を行い、そこから他のサイトへ同様な攻撃を繰り返すインターネットワーム（ワーム）など、殆どステップを踏まないものも多い。図８では、攻撃をステップ毎に５つのレベルに分類している。まず、各ステップについての攻撃手法、特徴及びＩＤＳログに残る痕跡について説明する。

【００８５】

攻撃のレベル１としては、「情報収集」がある。情報収集とは、ターゲットホスト探索のためのIPスキャン、ホストの脆弱性探索のためのPortスキャン及びFinger Printなどを試みる攻撃である。ＩＤＳログには、複数のIPへのアクセス及び複数のPortへのアクセスの痕跡が残る。他には、ハブ及びルータ上でのトラヒック盗聴などもあるが、これについてはＩＤＳ５０では通常検知できない。

【００８６】

攻撃のレベル２としては、「侵入の試み・脆弱スイープ」がある。侵入の試み・脆弱スイープとは、パスワードの辞書攻撃、コネクションハイジャック、プログラム上のバグや設計上の弱点を突くバッファオーバフロー攻撃及びエクスプロイト攻撃などである。広く出回っているワーム及び攻撃ツールによる攻撃の場合、同じパターンの痕跡が残る。

【００８７】

攻撃のレベル３としては、「侵入後の権限昇格・消去・改竄・盗聴・隠蔽」がある。侵入後の権限昇格・消去・改竄・盗聴・隠蔽とは、ローカル権限昇格、ハードディスク上のデータの消去、ホームページコンテンツ等の改竄、重要データの盗難、侵入後の証拠ログの隠蔽などである。ひとたび侵入を許してしまった場合には、本攻撃ステップと通常利用との区別をＩＤＳ５０によって行うことは困難であり、ログ５１に痕跡が残ることは殆どない。

【００８８】

攻撃のレベル４としては、「踏み台」がある。踏み台とは、侵入されたホストから他のホストへ攻撃を試みることである。特にワームに感染した場合には、外部の複数のホストから時々来ていた攻撃が、逆に外部の複数のホストを攻撃するようになり、多量のログが記録される。

【００８９】

攻撃のレベル５としては、「ＤＤos」がある。ＤＤosには、Smurf及びトロイの木馬プログラム等によるトラヒックオーバフロー攻撃がある。この場合、複数の外部ホストから特定の内部ホスト、または複数の内部ホストから特定の外部ホストに対して、同じパターンの痕跡が残る。

【００９０】

本実施形態のＩＤＳログ分析支援システム１は、レベル１の攻撃については、比率分析モデル又は閾値学習モデルにより、執拗に情報収集を行うSource IP（攻撃元）を抽出することができる。また、初検出モデルにより、新たに攻撃を試みたSource IPを把握できる。

【００９１】

また、ＩＤＳログ分析支援システム１は、レベル２の攻撃については内外類似度分析モデル、アクセス国分析モデル、比率分析モデル、閾値学習モデルによりインターネット上で新たに広がりをみせるワームの攻撃規模及び感染ホストについて、客観的な評価を行うことができる。

【００９２】

レベル３の攻撃ついては現在技術のＩＤＳ５０のログ５１に殆ど記録されないため期待できない。ただし、レベル３の攻撃ついてログ５１に記録できるＩＤＳ５０を用いることにより、ＩＤＳログ分析支援システム１によるレベル３の攻撃についての迅速な検出が可能となる。

【００９３】

また、ＩＤＳログ分析支援システム１は、レベル４の攻撃については内外類似度分析モデル、アクセス国分析モデル、比率分析モデル、閾値学習モデルにより、顕著に特徴を捉えることができる。

また、レベル５の攻撃については、ＩＤＳログ分析支援システム１の比率分析モデル及び閾値学習モデルが規模を把握するのに適している。

【００９４】

これらにより、本実施形態のＩＤＳログ分析支援システム１は、様々なＩＤＳ５０から出力される多量のログ５１をデータベース２０により統合的に管理して、ログ分析部３０により各種項目に関する統計的な分析を行うことができる。そこで、ＩＤＳログ分析支援システム１は、これまで運用者のスキルに依存していたネットワーク監視において、客観的な異常度を算出することができる。

【００９５】

すなわち、ＩＤＳログ分析支援システム１は、様々なＩＤＳ５０からのログ５

１を管理できる統合データベースを持ち、これに対する統計分析手段となるログ分析部３０が、長期プロファイルに対する短期プロファイルの差異を評価する統計値パターン分析モデル（内外類似度分析手段、アクセス国分析手段）、比率分析モデル（手段）、閾値学習モデル（手段）を備えている。これらの統計分析手段を用いることで、誤検知及び多重検知などの冗長なログを多く含むログ５１の中から、執拗に攻撃してくる侵入者、インターネット上で新た出現した攻撃、ワーム感染及び踏み台化ホストなどを迅速に発見することができる。

【００９６】

以上、本発明の実施形態について図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。

【００９７】

上記実施形態のＩＤＳログ分析支援システムは、当該ＩＤＳログ分析支援システムの動作・機能をコンピュータを介して実行させるＩＤＳログ分析支援プログラムとして実現してもよい。ここで、「コンピュータ」は、WWWシステムを利用している場合であればホームページ提供環境（あるいは表示環境）も含むものとする。また、上記ＩＤＳログ分析支援プログラムは、このプログラムを記憶装置等に格納したコンピュータから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記ＩＤＳログ分析支援プログラムは、前述した機能の一部を実現するためのものであってもよい。さらに、前述した機能をコンピュータにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

【００９８】

【発明の効果】

以上説明したように、本発明によれば、様々なＩＤＳより大量に出力されたログの中から、普段と異なるログを迅速に抽出して、その異常度を客観的に評価す

ることができる。

【図面の簡単な説明】

【図１】　本発明の実施形態に係るＩＤＳログ分析支援システムを示す模式図である。

【図２】　同上システムで分析されるログの一例を示す表示例図である。

【図３】　同上システムのデータベースにおける事象テーブルを示す図である。

【図４】　同上データベースにおけるシグネチャテーブルを示す図である。

【図５】　同上データベースの事象パラメータテーブルを示す図である。

【図６】　同上システムの比例分析モデル（手段）の説明図である。

【図７】　同上システムの閾値学習モデル（手段）の説明図である。

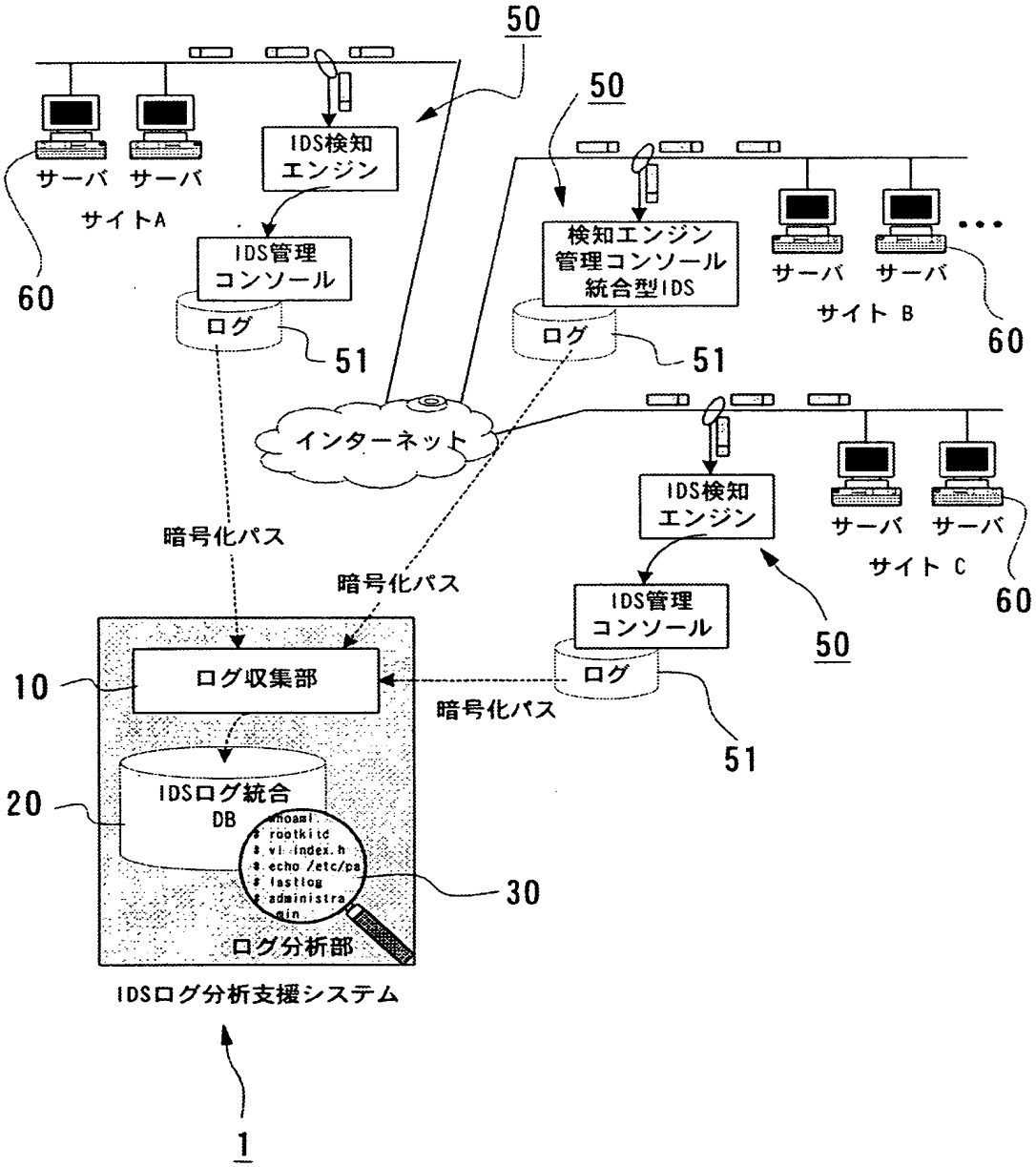
【図８】　各種の攻撃形態を示す説明図である。

【符号の説明】

１；ＩＤＳログ分析支援システム、１０；ログ収集部、２０；データベース、３０；ログ分析部、５０；ＩＤＳ、５１；ログ、６０；サーバ

【書類名】　図面

【図１】


50
50
IDS検知
エンジン
サーバ
サーバ
サイトA
IDS管理
コンソール
ログ
60
51
検知エンジン
管理コンソール
統合型IDS
ログ
51
サーバ
サーバ
サイト B
60
インターネット
IDS検知
エンジン
サーバ
サーバ
サイト C
60
暗号化パス
暗号化パス
IDS管理
コンソール
ログ
50
51
暗号化パス
10
ログ収集部
20
IDSログ統合
DB
30
ログ分析部
IDSログ分析支援システム
1

【図２】

```
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/21-19:23:53.643852  192.168.1.10:1086 -> 192.168.2.20:161
TCP TTL:128 TOS:0x0 ID:164 IpLen:20 DgmLen:48 DF
******S* Seq: 0x480DBF7C  Ack: 0x0  Win: 0xFAF0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
[Xref => cve CAN-2002-0013][Xref => cve CAN-2002-0012]
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/21-19:23:53.644145  192.168.1.10:1087 -> 192.168.2.20:162
TCP TTL:128 TOS:0x0 ID:165 IpLen:20 DgmLen:48 DF
******S* Seq: 0x480E4F26  Ack: 0x0  Win: 0xFAF0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
[Xref => cve CAN-2002-0013][Xref => cve CAN-2002-0012]
```

【図３】

Event ID	IDS IDS	Signature ID	Time	Source IP	Source Port	Destination IP	Destination Port	IP Protocol
1	1	26	2002/5/3 5:42	192.168.10.33	5963	127.0.0.137	53	UDP
2	1	12	2002/5/3 5:45	192.168.10.33	1766	127.0.0.138	5631	TCP
3	1	16	2002/5/3 5:45	127.0.0.140	1767	192.168.45.34	111	TCP
4	1	3	2002/5/3 5:45	192.168.10.36	1935	127.0.0.139	12345	TCP
5	1	11	2002/5/3 5:45	192.168.10.37	1972	127.0.0.140	53	TCP
6	1	102	2002/5/3 5:45	192.168.10.38	1977	127.0.0.141	698	TCP
7	1	301	2002/5/3 5:45	192.168.10.39	3333	127.0.0.142	137	TCP
8	2	302	2002/5/3 5:45	192.168.10.38	2222	127.0.0.141	138	TCP
9	2	26	2002/5/3 5:48	192.168.10.38	1111	127.0.0.141	53	UDP
10	2	526	2002/5/3 5:48	192.168.10.38	60171	127.0.0.141	80	TCP
11	1	301	2002/5/3 5:48	127.0.0.141	2002	192.168.10.38	-1	TCP
12	2	526	2002/5/3 5:48	192.168.10.38	60171	127.0.0.141	80	TCP
13	2	17	2002/5/3 5:48	192.168.10.38	3317	127.0.0.141	1080	TCP
14	2	18	2002/5/3 5:48	192.168.10.38	3391	127.0.0.141	1723	TCP
15	1	102	2002/5/3 5:48	127.0.0.142	3415	192.168.0.12	385	TCP
16	1	301	2002/5/3 5:48	192.168.10.35	5963	127.0.0.139	137	TCP

【図４】

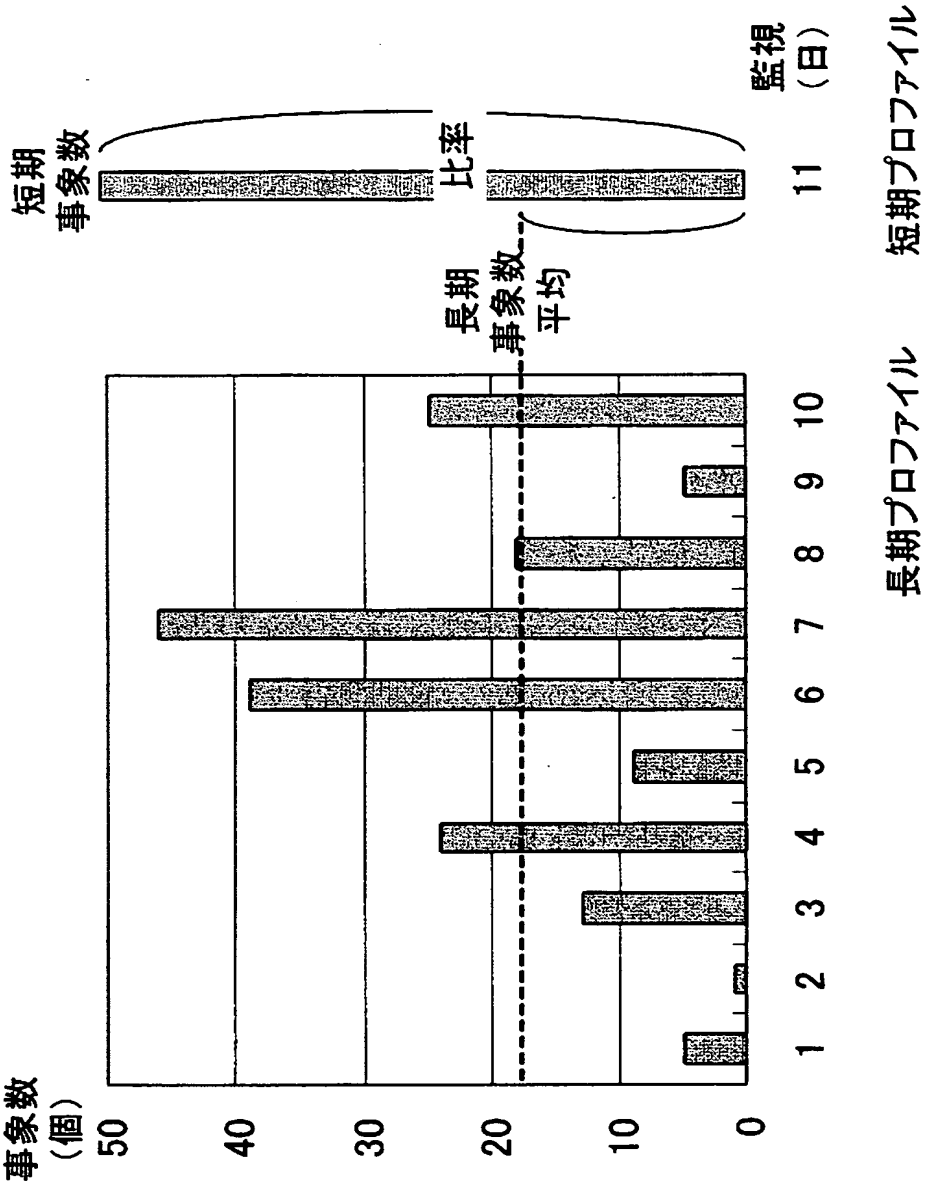
IDS	Signature	Signature		
ID	ID	Name		Severity
1	1	TCP port probe		1
1	2	UDP port probe		1
1	3	PCAnywhere port probe		1
1	4	RPC TCP port probe		1
1	5	NetBus port probe		2
1	6	DNS TCP port probe		1
1	7	DNS UDP port probe		1
1	8	TCP port scan		2
1	9	UDP port scan		2
1	10	TCP SYN flood		3
1	11	Telnet port probe		2
1	12	NMAP ping		3

【図５】

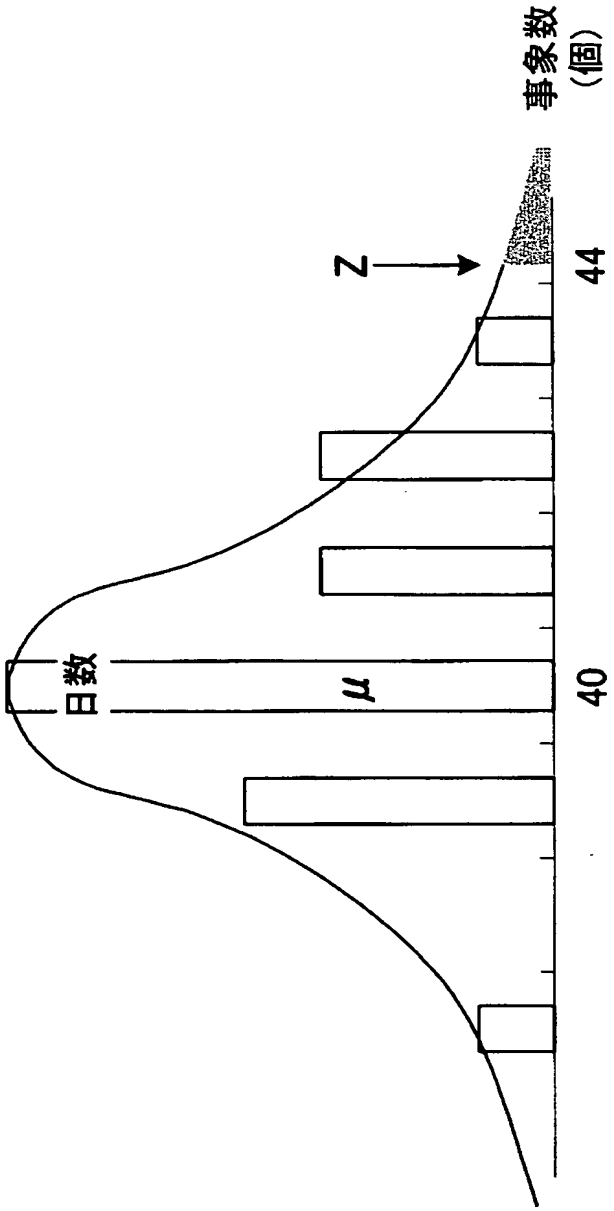
Event ID	Parameter	
	Name	Value
2	port	5631
2	reason	RSTsent
3	port	111
3	reason	RSTsent
4	port	12345
4	name	NetBus
4	reason	RSTsent
5	port	53
5	reason	RSTsent
6	port	1-93, 131-403, 441-723, 765-1019, 1067-1110, 1248, 1356
6	reason	RSTsent
7	port	2-3, 5, 8-9, 11-15, 17, 19-21, 23-28, 30-32, 35-36, 40-43,
8	PercentFromIntruder	99-100
8	SYNs	214
8	DATAs	0
10	count	2

出証特２００４－３０２４８５１

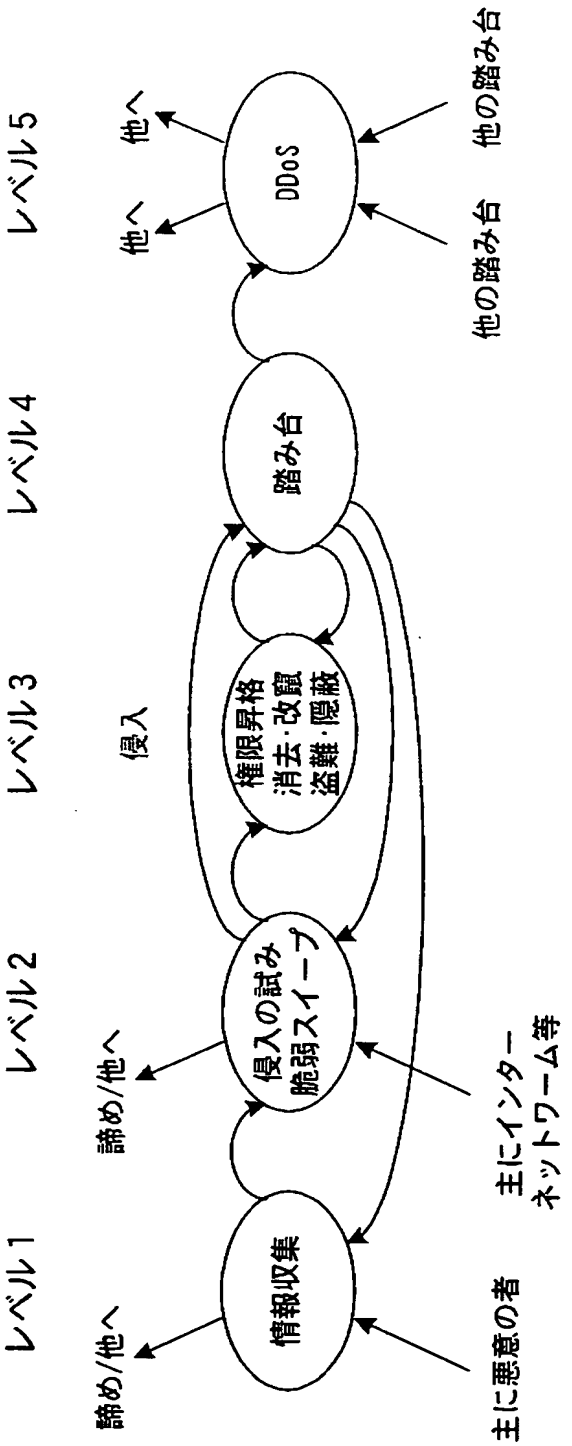
【図６】


事象数（個）
50
40
30
20
10
0
1 2 3 4 5 6 7 8 9 10 11
監視（日）
長期プロファイル
短期プロファイル
長期事象数平均
短期事象数
比率

【図７】



【図８】


レベル１
レベル２
レベル３
レベル４
レベル５
情報収集
侵入の試み
脆弱スイープ
権限昇格
消去・改竄
盗難・隠蔽
踏み台
DDoS
侵入
諦め/他へ
諦め/他へ
他へ
他へ
主に悪意の者
主にインター
ネットワーム等
他の踏み台
他の踏み台

【書類名】　　要約書

【要約】

【課題】　様々なＩＤＳより大量に出力されたログの中から、普段と異なるログを抽出して、その異常度を客観的に評価することができるＩＤＳログ分析支援装置、ＩＤＳログ分析支援方法及びＩＤＳログ分析支援プログラムを提供する。

【解決手段】　通信網に接続されたＩＤＳ５０のログ５１を収集するログ収集部と１０、ログ収集部１０で収集されたログについて保存して管理するデータベース２０と、データベース２０で管理されているログについて統計をとり分析処理するログ分析部３０とを有することを特徴とする。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００３－１１２４１４
受付番号	５０３００６３４８３８
書類名	特許願
担当官	末武　実　　１９１２
作成日	平成１５年　４月２４日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000208891
- 【住所又は居所】 東京都新宿区西新宿二丁目３番２号
- 【氏名又は名称】 ＫＤＤＩ株式会社

【代理人】 申請人
- 【識別番号】 100101465
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 青山　正和

【代理人】
- 【識別番号】 100064908
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 志賀　正武

【選任した代理人】
- 【識別番号】 100089037
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 渡邊　隆

次頁無

特願２００３－１１２４１４

出　願　人　履　歴　情　報

識別番号　［０００２０８８９１］

１．変更年月日　２００２年１１月２８日
［変更理由］　名称変更
住　所　東京都新宿区西新宿二丁目３番２号
氏　名　ＫＤＤＩ株式会社